2021

Server Management Code of Practice

ISSUE 1.0

TECHNICAL SECURITY TEAM

Contents

1.0 Purpose

The purpose of this Code of Practice is to outline the requirements for securely managing servers within the University – minimising vulnerabilities that put University data, systems and infrastructure at risk of cyber-attack, compromise and loss. This document outlines the technical security baseline requirements, based on the University Information Security Policy and regulatory requirements including: Data Protection Act 2018, Cyber Essentials certification[i], National Cyber Security Centre and JISC security Policy and guidance; as well as the requirements of our collaboration partners.

2.0 Scope and Approach

The Code of Practice applies to both physical and virtual servers, whether provided and managed by the IT Services Department or sourced and managed independently by departments. It applies to all members of the University including students, staff and Honoraries, as well as associate and third-party suppliers. It describes the following:

- Security Principles underpinning effective Server management
- Protection measures that Business Owners and System Owners/System Administrators should apply to protect their information and the University environment.
- Security and support from IT Services that helps achieve the principles of this Code of Practice.

3.0 Security Principles: Know what you have, protect it, govern and review it

Effective server management relies on the principles of ownership, inventory management, risk management (by Owners and IT Services) and regular maintenance and review.

Inventory: Inventory of IT assets connected to the network is recorded and kept, including local servers, network or storage devices locally or centrally procured, used or maintained. The asset inventory will help IT Services to work with Business Owners to build in reviews and risk management to establish and maintain a secure operating environment.

Ownership: Ownership describes the person most operationally responsible for the service (as per Information Security Policy). The following are key ownership roles:

- **Business Owner:** The senior person responsible and accountable for the service (e.g. Dean, Head of Department, Principal Investigator etc.).
- **System Owner/Administrator:** Role in charge of and responsible for managing the systems which provide the service. This includes implementing baseline technical security measures.

Protection measures: These represent the baseline technical security measures the Business Owner and System Owner/Administrator should implement, as outlined in section 4.0. Centralised support, monitoring and incident response are available from IT Services, as described in section 5.0.

Governance and review: This involves a process of regular review of the IT asset inventory to ensure it is accurate and reliable, and that any changes or updates to servers are reflected in inventory. Only IT assets which have an ongoing business justification should remain in operation. The business justification of servers within the estate should be reviewed annually and revalidated by owners. Servers and networked storage which are no longer needed should be identified by this process and decommissioned through to secure disposal in a timely manner.

4.0 Technical Protection responsibilities for Business & System Owners

This section outlines technical security controls which constitute the baseline minimum protection measures which should be implemented by Business Owners and System Owners/Administrators. A description of each control is given in the left-hand column, while specific ownership responsibilities are listed on the right.

Technical security Control area	Business Owner and System Owner responsibilities
Server registration and IT asset inventory Capturing the owner and responsible roles. Description of data and sensitivity / data classification. May include: contractual / regulatory requirements e.g. Cyber Essentials, NHS DSPT, GDPR etc. Whether external, off-campus connectivity is required	• Server registration and annual review / revalidation of inventory. • Notifying IT Services of the transfer in ownership of any IT assets. • Work with IT Services to identify and implement security controls (technical and organisational) in accordance with legislative, regulatory and contractual requirements.
Patching Suppliers release periodic updates (patches) to operating systems and applications to resolve bugs and security vulnerabilities. Failure to fund and maintain operating system and software patches increase the server vulnerability to attack, which increases vulnerability of the University network as a whole. Patches flagged as '*critical*' or '*security*' updates should be installed without delay.	• Monitor the release schedules of updates to the operating systems and applications which run on their servers. • Assess and record the impact of installing the update. • Speak to IT Services for advice and to develop a risk management plan when standard patching and updates may not be feasible.
Security tools Device level tools providing an extra layer of defence against threats. These include: anti-malware and Security Information and Event management (SIEM) tools, which detect, report and mitigate threats within the network, overseen by the Security Operations Centre (SOC) within the IT Services Technical Security Team.	• Ensuring anti-malware is installed on their servers. • Ensuring that SIEM agent software is installed and reporting into the SOC. • Responding to security alerts which are generated by security tools or the SOC.
Network and firewall Connectivity In order to protect the University network as a whole it is essential to monitor and record connections which are permitted in and out of the campus infrastructure, including internet connections. This is managed by network security infrastructure including firewalls which block or allow connections based on rules. This includes the following controls: • Security review of requests for new external connectivity • Assigning ownership of firewall rules which permit external connectivity. • Review and revalidation of firewall rules on a regular basis. Disabling firewall rules which allow access which is no longer needed.	• Don't put anything on the network until it has been reviewed by the Technical Security team. • Complete the server (or NAS) registration process including network and firewall connectivity requirements. • Work with IT Services to manage the security risks of connections to owned servers and services. • Review and revalidate firewall rules on a regular basis. • Notify IT Services when firewall rules are no longer required.
Access Management and passwords Access management defines the measures taken to enable access to servers and to ensure that this is restricted to those with a legitimate business purpose, that access is the	• Validate business need of user accounts prior to granting access. • Always apply the principle of 'minimum privilege'. • Review accounts regularly and disable when no longer required.

Technical security Control area	Business Owner and System Owner responsibilities
minimum level necessary, is regularly reviewed and removed when no longer necessary. Password controls, including complexity rules and changing of default passwords are minimum requirements.	• Apply password management: ○ Change default 'out of the box' passwords ○ Enforce password complexity ○ Do not share passwords
Back-up Backup of data provides a means to restore the state of a service in the event of a serious incident which results in the loss of data held on a server. A backup strategy should consider the frequency that backups are taken, the media that data is backed up to and the location in which backed up data is held. IT Services can provide advice and recommendations on suitable backup strategies.	• Determining the backup requirements of owned servers. • Implementing suitable backup arrangements for requirements. • Ensuring that systems can be successfully restored from backup when required. • Discuss and request advice from IT Services as required.
Resilience/availability requirements Resilience addresses maintaining service in the event of a server failing or going offline. This includes powering devices and whether resilient power options such as a UPS (Uninterruptible Power Source) are required. Common approaches include: **High availability (HA):** Where multiple servers share the load of providing service. **Hot standby:** Where a second server automatically takes over in the event of a failure. **Warm/cold standby:** Where a second server can be manually enabled to take over. **No resilience:** Where the service becomes unavailable if the server fails. IT Services can advise on resilience and best practice for given services and deployments.	• Determining the level of resilience required for owned services. • Implementing the desired level of resilience. • Managing the risk associated with any outage on their servers. • Request advice from and discuss with IT Services the resilience options and good practice for given services and deployments.
Supplier Management Services which run on servers in the estate may incorporate the services, software or infrastructure of 3rd parties as part of their design. In such circumstances, the role of maintaining the 3rd party components of the service is usually held by the 3rd parties themselves and not University personnel. Where this is the case, server owners should maintain relationships with 3rd parties and ensure that any maintenance obligations are fulfilled as required.	• Maintaining the relationship with 3rd party suppliers. • Ensuring that appropriate maintenance arrangements are in place with 3rd party suppliers. • Ensuring that maintenance obligations (including patching) are completed as required by the service. • Request guidance from IT Services on appropriate technical expectations of 3rd party suppliers.

Please note: Server and NAS registration and Firewall connection request forms are included in the Hardware catalog in the IT self-service portal https://servicedesk.liverpool.ac.uk

5.0 Security & Support from IT Services

The IT Services Department hold overall responsibility for the delivery and management of IT within the institution. IT Services has a number of specialist teams with different responsibilities in respect of server management – including the Servers & Storage and Technical Security teams. IT Services responsibilities include the following:

- Carrying out vulnerability scans to identify any known vulnerabilities present within network connected assets (server/NAS etc) which need remediation.
- Receiving, coordinating and supporting the University-wide responses to security alerts.
- Managing the Security Operations Centre (SOC), including receiving, triaging and responding to security issues reported by University personnel.
- Conducting security reviews of new requests for firewall rules and network connections.
- Monitoring server inventory. Investigating and taking action if technical protection or ownership details are insufficient, or if the business justification is not validated.
- Deploying and managing security tools and the Security Information and Event Management (SIEM) capabilities, including (but not limited to):
    - Monitoring for anomalous user access attempts which may indicate a cyber-threat.
    - Receiving, correlating and analysing server logs to detect potential cyber-threats.
    - Ensuring that servers have appropriate technical security tooling installed.
- Supporting Business and System Owners with advice and responding to support requests on the technical protection measures outlined in section 4.0, above.

Compliance and Security incident response

The cyber security threat landscape creates day to day operational management challenges which often require a rapid, coordinated response to ensure that University systems and data are not compromised and remain available for their intended purpose. This often involves University-wide remedial action with IT Services in response to known threats, including:

- Liaising with law enforcement, the National Cyber Security Centre, intelligence partners and University leadership to understand the threat and its potential impact on the University.
- Notifying affected Owners and stakeholders of the details of the threat.
- Assessing impact to the University network and services, including remediation plans. This may include temporary disconnection of services as per the IT Acceptable Use Policy.
- Monitoring and reporting on the progress of remediation plans to senior management.
- Supporting Owners and other stakeholders with the detail of remediation or any queries relating to security threats.

6.0 Monitoring and Compliance

Owners and Administrators are urged to implement the controls described in this document as fully as practicable, and demonstrate a disciplined risk management approach when controls cannot be implemented. IT Services will take reasonable steps to measure compliance with controls for all servers on the network. Where servers fail to meet security best practices, IT Services will assist owners to remediate issues – reporting any persistent or serious failings to Senior Leadership. Where it is not possible to secure servers or reduce risks to a tolerable level, IT Services reserves the right to disconnect such servers from the network, until appropriate mitigation can be put in place.

7.0 Document control

Document Version Control			
Author	**Summary of Changes**	**Version**	**Approval (Role & date)**
Jimmy Tickle – Senior Security Analyst, IT Services	First issue - outline server management best practice.	1.0	Information Governance Committee 15/10/2021 Head of Infrastructure & Ops, IT Services 22 July 2021
Policy Ownership & Review			
Owner and contact for enquiries	This document is owned by the Head of Infrastructure and Operations of the IT Services Department. The IT Services Technical Security team are the document authors and initial point of contact for any enquiries is via the IT Service Desk at https://servicedesk.liverpool.ac.uk		
Review due:	1 September 2022		
Document location	https://www.liverpool.ac.uk/csd/regulations/		
** Owner & Author are responsible for communicating this policy document**			

[i] Cyber Essentials (https://www.ncsc.gov.uk/cyberessentials/overview) is a pre-requisite for organisations requesting Government funding for collaboration on research, development projects, and for collaboration with the NHS: requesting NHS health & care data for research.